In the Claims
(Clean Version Showing Claims as Amended)

1. A method for recognizing and refusing denial of service and distributed denial of service attacks on server systems of network providers and operators by means of an electronic intermediary device implemented in a computer network, wherein the electronic intermediary device contains a computer program for carrying out defense for a target computer system against the denial of service and distributed denial of service attacks, for each one of a network connection request, performing the following steps:

A1

registering the network connection request and storing a data packet associated with the network connection request in a computer memory;

checking the validity of the registered network connection request and the data packet associated with the network connection request, and while the data packet is being checked for validity;

sending a periodic acknowledgement signal to preserve the network connection between the target system and the network connection request, and after receiving confirmation of the validity of the network connection request;

forwarding the data packet associated with the network connection request to the target system which was the subject of the network connection request.

2. A method according to claim 1, further comprising the step(s) of:

checking for an available network service in the target system which can receive the data packet.

A2 Cont

3. A method according to claim 2, wherein if the network connection request and the data packet are deemed valid, and the available network service is available, then prior to performing the step of forwarding the data packet, performing at least one of the following steps:

receiving the data packet directly from a data link level;

examining a file header of the data packet and rejecting the data packet if the file header contains an invalid value;

examining a length value and a checksum value of the data packet and comparing said length value and said checksum to a corresponding pair of values resident in the file header and rejecting the data packet if said length value and said checksum value are different from the corresponding pair of values;

for an answering message from the target system to a requesting system from which the network connection request originates, using a neutralizing protocol identifier so that an actual TCP/IP fingerprint of the target system is not sent to the requesting system;

for avoiding such attacks upon the target system via a network protocol user datagram protocol, selectively registering and blocking each of a set of network services of the target system that are not required to be reached via user datagram protocol;

A2 cont.

for all data packets of an internet control message protocol type, rejecting the data packet if it has a length value that exceeds a predefined maximum length value; or

comparing the internet protocol address of the requesting system to a listing of invalid internet protocol addresses, and excluding the data packet if the internet protocol address of the requesting system appears on the listing of invalid internet protocol addresses.

4. A method of according to claim 3, wherein for each data packet of an internet control message protocol type, instead of rejecting the data packet if it has a length value that exceeds a predefined maximum length value, performing the following step:

reducing the length value to an approved value wherein said approved value is equal to or less than the predefined maximum length value.

5. A method according to claim 3, for each data packet of an internet control message protocol type, blocking the data packet if the data packet is a single type of several possible types of such internet control message protocol type.

6. A method according to claim 5, further comprising the step of first:

establishing an administrative operating network node coupled to the target system which is accessible from either a single secure console location or via a secure network connection.

7. A method according to claim 6, further comprising the step of limiting the amount of time that the target system is accessible to receive the network connection request.

8. In a computer system, a computer-readable storage media storing at least one computer program that operates to recognize and refuse attacks on computer networks, comprising the steps of:

registering a network connection request and storing a data packet associated with the network connection request in a computer memory;

A2 cm't

checking the validity of the registered network connection request and the data packet associated with the network connection request, and while the data packet is being checked for validity;

sending a periodic acknowledgement signal to preserve the network connection between the target system and the network connection request, and after receiving confirmation of the validity of the network connection request; and

forwarding the data packet associated with the network connection request to the target system which was the subject of the network connection request.

9. A method according to claim 8, further comprising the step of:

checking for an available network service in the target system which can receive the data packet.

10. A method according to claim 9, wherein if the network connection request and the data packet are deemed valid, and the available network service is available, then prior to performing the step of forwarding the data packet, performing at least one of the following steps:

receiving the data packet directly from a data link level;

examining a file header of the data packet and rejecting the data packet if the file header contains an invalid value;

examining a length value and a checksum value of the data packet and comparing said length value and said checksum to a corresponding pair of values resident in the file header and rejecting the data packet if said length value and said checksum value are different from the corresponding pair of values;

for an answering message from the target system to a requesting system from which the network connection request originates, using a neutralizing protocol identifier so that an actual TCP/IP fingerprint of the target system is not sent to the requesting system;

for avoiding such attacks upon the target system via a network protocol user datagram protocol, selectively registering and blocking each of a set of network services of the target system that are not required to be reached via user datagram protocol;

A2 con't

for all data packets of an internet control message protocol type, rejecting the data packet if it has a length value that exceeds a predefined maximum length value; or

comparing the internet protocol address of the requesting system to a listing of invalid internet protocol addresses, and excluding the data packet if the internet protocol address of the requesting system appears on the listing of invalid internet protocol addresses.

11. A method of according to claim 10, wherein for each data packet of an internet control message protocol type, instead of rejecting the data packet if it has a length value that exceeds a predefined maximum length value, performing the following step:

reducing the length value to an approved value wherein said approved value is equal to or less than the predefined maximum length value.

12. A method according to claim 10, for each data packet of an internet control message protocol type, blocking the data packet if the data packet is a single type of several possible types of such internet control message protocol type.

13. A method according to claim 12, further comprising the step of first:

establishing an administrative operating network node coupled to the target system which is accessible from either a single secure console location or via a secure network connection.

14. A method according to claim 13, further comprising the step of limiting the amount of time that the target system is accessible to receive the network connection request.

15. A data carrier containing a computer program for recognizing and refusing attacks on server systems of network service providers and operators via use of an electronic device coupled to a computer network, said computer program comprising the steps of:

A2 cont

registering the network connection request and storing a data packet associated with the network connection request in a computer memory;

checking the validity of the registered network connection request and the data packet associated with the network connection request, and while the data packet is being checked for validity;

sending a periodic acknowledgement signal to preserve the network connection between the target system and the network connection request, and after receiving confirmation of the validity of the network connection request;

forwarding the data packet associated with the network connection request to the target system which was the subject of the network connection request; and

checking for an available network service in the target system which can receive the data packet.

16. The data carrier of claim 15, further comprising:

a non-network-addressed electronic intermediary device passively coupled to a computer network, wherein said electronic intermediary device monitors each data packet received by the computer network which data packet contains a network connection request.

17. The data carrier of claim 15, wherein the computer program further comprising the steps of:

registering each of a plurality of network connection requests to a target network system;

answering each of the plurality of network connection requests with an acknowledgement signal, wherein the acknowledgement signal meets a timeout criteria for the target network system;

checking the validity of the registered network connection request;

checking for an available service in the target system;

initializing a connection to the target system; and

if validity of the registered network connection request is confirmed, forwarding a consecutively following data packet, which data packet is associated with the network connection request, to the target system for further processing.

A2 cont.

18. The data carrier of claim 17, wherein prior to forwarding the data packet to the target system, performing at least one of the following steps:

examining a header of the data packet and rejecting the data packet if the header contains invalid data;

examining a length value and a checksum value for conformity to corresponding values contained in the header of the data packet;

replacing an actual network fingerprint data of the target system with a default network fingerprint protection data;

selectively registering all user datagram protocol-compliant ports of the target system and forwarding the data packet if it contains or comprises a user datagram protocol network packet addressed to a datagram protocol-compliant port and blocking each data packet that contains a user datagram protocol network packet if it is addressed to port that is not compliant with a user datagram protocol;

identifying the data packet as valid if the data packet meets a predefined maximal Internet control message protocol length, and rejecting the data packet if the data packet exceeds the predefined maximal Internet control message protocol length others are rejected;

excluding a specific external network source-address from the communication with the target system;

examining all incoming and outgoing data packets for compliance with at least one of a group of user defined-rules, rejecting each of the data packets that do not comply with said at least one of the group of user-defined rules, and forwarding each of the data packets which comply with said at least one of the group of user-defined rules;

excluding a predefined network user from a set of otherwise available services of the target system;

excluding a predefined network service from the set of otherwise available services of the target system; or

A2 concld.

redirecting the network connection request.

19. The data carrier of claim 15, wherein said computer program is stored in a programmable read-only memory storage location.

20. The data carrier of claim 18, wherein the target system is connected to a distributed network such as a internet, intranet, extranet or the like, and said target system contains at least one computer configured as server computer and at least one computer configured as a client computer and a data line to be protected from denial of service attacks is equipped with an electronic intermediary device which is switched between the target network, the server computer or the client computer.